⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2−151892

⑤Int.Cl.⁵	識別記号	庁内整理番号	㊸公開　平成2年(1990)6月11日
G 09 C 1/00		7368−5B	
G 06 F 7/72		7056−5B	

審査請求　未請求　請求項の数 1　(全11頁)

㊹発明の名称　べき乗剰余演算装置

㉑特　願　昭63−307361
㉒出　願　昭63(1988)12月5日

㉗発明者　松崎　なつめ　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉗発明者　館林　誠　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉔代理人　弁理士　粟野　重孝　外1名

明　細　書

1．発明の名称

べき乗剰余演算装置

2．特許請求の範囲

素数pと素数qの積nを法とし、正整数dをべき数として入力xのべき乗剰余演算を行う装置であり、前記正整数dと素数qの値を保持し、かつその値が外部から決定あるいは推測できないように構成された第1の計算装置と、この第1の計算装置から送出された第1のデータに対して所定の計算を行いその結果を第2のデータとして前記第1の計算装置に送出する第2の計算装置からなり、前記第1の計算装置は前記素数pとqの積nと、前記正整数dをp−1で除した剰余d1と、前記正整数dをq−1で除した剰余d2を計算してこれらの結果を前記第1のデータとして前記第2の計算装置に送出し、さらに前記第2の計算装置から送出された前記第2のデータを前記素数pとqを用いて結合し、法を前記の数nとし、前記正整数dをべき数とする入力xのべき乗剰余値を求めるものであり、前記第2の計算装置は前記第1の計算装置から送出された前記第1のデータから、前記整数nを法とし前記d1をべき数とする前記正整数xのべき乗剰余数y1と、前記整数nを法とし前記d2をべき数とする前記正整数xのべき乗剰余数y2を計算し、この結果を前記第2のデータとして前記第1の計算装置に対して送出することを特徴とするべき乗剰余演算装置。

3．発明の詳細な説明

産業上の利用分野

本発明はICカードなど計算能力のあまり高くないデバイスが補助装置を用いてRSA暗号などの公開鍵暗号の基本演算であるべき乗剰余演算を行うべき乗剰余演算装置に関するものである。

従来の技術

RSA暗号を代表とする公開鍵暗号方式は

① 鍵配送が容易である。

② 秘密に保持する鍵の種類が少ない。

③ 安全な認証機能（ディジタル署名機能）がある。

などの長所を持つ反面、その安全性を保証するためには例えば５１２ビット程度の長語長の数のべき乗剰余演算、すなわちｙ＝ｘ＾ｄ　ｍｏｄｎ（ｘ，ｄ，ｎ：５１２ビット）を行う必要がある。なお、ここで'＾'はべき乗演算を示し、ｍｏｄｎはｎで除したときの剰余を示す。以降これらの記述を用いる。

この長語長の演算を例えば８ビットや１６ビットの汎用ＣＰＵのソフトウェアで実現すると、数１０秒といった非常に長い演算時間を要す。

一方、ＩＣカードは計算・記憶・情報保護能力を備え、携帯に便利なデバイスであり、特に金融関係に有望である。ＩＣカードを金融関係に用いる場合、送られてきた暗号文の送信者が偽者でないことを確認できる認証機能が特に重要になってくる。前記したように公開鍵暗号方式は安全な認証機能を有し、この点でＩＣカードにおいて公開鍵暗号方式を実現する義務がある。ところがＩＣカードの計算能力，記憶能力はあまり高くなく、前述したように膨大な演算量を必要とする公開鍵暗号方式をＩＣカード単独で実現することは実用上不可能である。そこでこの基本演算であるべき乗剰余演算を計算能力，記憶能力のすぐれている補助装置（たとえばＰＯＳ端末など）の助けをかりて行うことを考える。ただし、この補助装置は必ずしもＩＣカードにとって信頼できるものではないため、ＩＣカード内の秘密の情報は漏らさないことが必要である。この方法を「補助装置を用いたべき乗剰余演算装置」と称する。

従来の補助装置を用いたべき乗剰余演算装置としてはたとえば文献「加藤，松本"安全な計算依頼法について"１９８８年暗号と情報セキュリティシンポジウム」に示されている。

第２図に従来のべき乗剰余演算装置における第１の例の構成図を示す。１００はＩＣカード、１０１は補助装置である。１０２，１０３はそれぞれＩＣカードにおける秘密のデータｐ，ｑを格納しているｐ格納部とｑ格納部、１０４はｐとｑの積を計算してｎを生成するｎ生成部、１０５はｎを公開するｎ公開部である。１０６はＩＣカー

$$y_i = x^{d_i} \bmod n \quad (i = 1 \sim m) \quad \cdots\cdots(2)$$

１１６は前記Ｙ'をＩＣカードに送信するＹ'送信部である。１１７はＩＣカード内でＹ'を受信するＹ'受信部、１１８は前記Ｙ'，ｎ，Ｆを用いて(3)式の計算を行いｙを生成するｙ生成部である。

$$y = (y_1^{f_1}) \times \cdots\cdots \times (y_m^{f_m}) \bmod n \quad \cdots\cdots(3)$$

１１９は前記ｙを格納するｙ格納部である。

なお、前記１０２～１１１，１１７～１１９はＩＣカードを１００に含まれ、１１２～１１６は補助装置に含まれる。また、１０２～１０９，１１２～１１３は初期化のときのみに動作する。

次に、以上説明した従来のべき乗剰余演算装置の動作を、ＲＳＡ暗号の復号化を行う場合を例に説明する。

＜ＲＳＡ暗号の復号化＞

ｘを５１２ビットの暗号文、ｄを秘密の復号化鍵（５１２ビット）、ｎを５１２ビットの公開値とするとき、以下の(4)式の演算を行うことによっ

ドにおける秘密のデータｄを格納しているｄ格納部、１０７はｄを次の(1)式のように表現し、これを満たすＤ＝{ｄ１，……，ｄｍ}，Ｆ＝{ｆ１，……，ｆｍ}を求めるｄ分割部である。

$$d = d_1 \times f_1 + \cdots\cdots + d_m \times f_m \bmod \lambda(n) \quad \cdots\cdots(1)$$

ただし、λ(n)はｐ－１とｑ－１の最小公倍数とする。

また、ｄｉ＜（ｐ－１）×（ｑ－１），ｆｉ＝１または０　（ｉ＝１～ｍ）である。

１０８は前記Ｄを補助装置１０１に送信するＤ送信部，１０９は前記Ｆを格納するＦ格納部である。１１０はデータｘを格納しているｘ格納部，１１１はｘを補助装置に送信するｘ送信部である。１１２は補助装置内で公開数ｎを受信するｎ受信部、１１３，１１４はそれぞれＩＣカードからのＤ、ｘを受信するＤ受信部，ｘ受信部である。１１６は１１２～１１４のデータを用いて次の(2)式を計算してＹ'＝（ｙ１，……，ｙｍ）を求めるべき乗剰余計算部である。

7 ページ

て５１２ビットの復号文ｙを得る。

$$y = x^{d} \bmod n \quad (x, d, n：512ビット) \quad \cdots\cdots(4)$$

ただし、ｎ＝ｐ×ｑ（ｐ，ｑ：２５６ビットの素数）であり、このＲＳＡ暗号の復号化を行う主体であるＩＣカードだけはｎの素因数分解ｐ，ｑを知っているとする。

＜初期化＞

① ＩＣカード内のｐ，ｑ（ＩＣカードの秘密の情報）がそれぞれｐ格納部１０２，ｑ格納部１０３に格納されている。ｎ生成部１０４においてｐとｑの積を計算してｎ公開部１０５に格納する。ｎはこのｎ公開部１０５により広く公開される。

② ＩＣカード内のｄ（ＩＣカードの秘密の情報）がｄ格納部１０６に格納されている。ｄ分割部１０７においてｄを前記(1)式のように表現し、これを満たすＤ＝｛ｄ１，……，ｄｍ｝，Ｆ＝｛ｆ１，……，ｆｍ｝を求める。ただしここでｄｉ＜（ｐ－１）×（ｑ－１），ｆｉ＝１またはＯである。

Ｄはｄ送信部１０８より補助装置に送信される。

ＦはＩＣカード内のＦ格納部１０９に格納される。

③ 補助装置内のｎ受信部１１２は公開されているｎを受信する。

④ 補助装置内のＤ受信部１１３はＩＣカードより送信されたＤを受信する。

＜繰り返し処理＞

以下の処理は５１２ビットを１ブロックとする暗号文の数だけ繰り返す。

① 暗号文１ブロックをＩＣカード内のｘ格納部に格納する。

② ＩＣカード内のｘ送信部１１１より補助装置内のｘ受信部１１４に暗号文ｘを送信する。

③ 補助装置のべき乗剰余計算部１１５は暗号文ｘ，公開値ｎ，ＩＣカードから受け取ったＤを用いて前記(2)式の演算を行い、Ｙ′＝｛ｙ１，……，ｙｍ｝を得る。

④ 補助装置内のＹ′送信部は前記べき乗剰余計算

9 ページ

部１１５の出力をＩＣカード内のＹ′受信部１１７に送信する。

⑤ ＩＣカード内のｙ生成部１１８は補助装置が求めたＹ′とＦ格納部に格納されているＦを用いて前記(3)式を計算する。

(3)式は補助装置が計算したＹ′＝｛ｙ１，……，ｙｍ｝のうち対応するＦ＝｛ｆ１，……，ｆｍ｝が“１”であるものを法ｎで乗算してｙを得ることを意味している。

なお、上記の方法で求めたｙは(4)式を満たしているｎ未満の正整数である。それは次の(6)より明らかである。

前記(3)式

$$= (y_1^{f_1}) \times \cdots\cdots \times (y_m^{f_m}) \bmod n$$

$$= (x^{d_1} \bmod n)^{f_1} \times \cdots\cdots \times (x^{d_m})^{f_m} \bmod n$$

$$= x^{(d_1 \times f_1 + \cdots\cdots + d_m \times f_m \bmod \lambda(n))} \bmod n$$

$$= x^{d} \bmod n \quad \cdots\cdots(5)$$

10 ページ

また、補助装置が総当たりによってＩＣカードの持つ秘密の鍵ｄの探索を行う場合、その鍵の候補数は、Ｆ＝｛ｆ１，……，ｆｍ｝のうちｆｉ＝１となるｉの個数をＬ以下にする場合、

$$\Sigma (i = 1 \sim L + 1)\ {}_mC_i$$

となる。ここでｍＣｉはｍ個のなかからｉ個を選ぶ組合せの数である。従って例えばＬを１５とした場合、その候補数は約１０　３０程度となり、実用上安全であると言える。しかしながら、この方法の場合、繰り返し処理におけるＩＣカードと補助装置の間の通信量が多く、ＩＣカードにおける計算量も大きい。１ブロック５１２ビットの暗号化に要する、ＩＣカードと補助装置の間の通信量はｍ＋１ブロックである。また、ＩＣカードにおける計算は最大ｍ回の法ｎ上の乗算が必要である。なお、ｍはＩＣカードの秘密データｄの安全性を決定しているパラメータである安全性の面より１６程度にする必要がある。このため、１ブロックの暗号化速度はＩＣカード単独で実現する場合に比べてせいぜい一桁高速になるだけである。

11

そこで、ＩＣカードと補助装置の間の通信量を減少して１ブロックの暗号化時間を短縮する方法も同文献において提案されている。

第３図に従来のべき乗剰余演算装置における第２の例の構成図を示す。１２０はＩＣカード、１２１は補助装置である。１２２，１２３はそれぞれＩＣカードにおける秘密のデータｐ，ｑを格納しているｐ格納部とｑ格納部、１２４はｐとｑの積を計算してｎを生成するｎ生成部、１２６はｎを公開するｎ公開部である。１２６はｐ，ｑより次の(6)，(7)式を満たすｗｐ，ｗｑを生成して格納するｗｐ，ｗｑ生成部である。

$$wp = q \times (q^{-1} \bmod p) \bmod n \quad \cdots\cdots(6)$$

$$wq = p \times (p^{-1} \bmod q) \bmod n \quad \cdots\cdots(7)$$

１２７はある秘密の数Ｒを格納するＲ格納部、１２８は前記ｐ，ｑ，Ｒを用いて次の(8)，(9)を満たすｒｐ，ｒｑを生成して格納するｒｐ，ｒｑ生成部である。

$$rp = R^{-1} \bmod (p-1) \quad \cdots\cdots(8)$$

$$rq = R^{-1} \bmod (q-1) \quad \cdots\cdots(9)$$

１２９はＩＣカードにおける秘密のデータｄを格納しているｄ格納部、１３０は前記ｄ，Ｒを入力として次の(10)式を満たすｄ′を生成するｄ′生成部である。

$$d' = d \times R \bmod \lambda(n) \quad \cdots\cdots(10)$$

１３１は前記ｄ′を補助装置に送信するｄ′送信部である。１３２はデータｘを格納しているｘ格納部、１３３はｘを補助装置に送信するｘ送信部である。１３４は補助装置内で公開値ｎを受信するｎ受信部、１３５，１３６はそれぞれＩＣカードより送られてきた前記ｄ′，ｘを受信するｄ′受信部，ｘ受信部である。１３７は前記１３４～１３６の各データを用いて次の(11)式の計算を行いｙ′を求めるべき乗剰余計算部である。

$$y' = x^{d'} \bmod n \quad \cdots\cdots(11)$$

１３８は前記ｙ′をＩＣカードに送信するｙ′送

13

信部である。１３９は前記ｙ′送信部より送られてきたｙ′を受信するＩＣカード内のｙ′受信部である。１４０は前記ｙ′，ｗｐ，ｗｑ，ｒｐ，ｒｑより次の(12)式を満たすｎ以下の数ｙを生成するｙ生成部である。

$$y = \{((y' \bmod p)^{rp} \bmod p) \times wp + ((y' \bmod q)^{rq} \bmod q) \times wq\} \bmod n \quad \cdots\cdots(12)$$

１４１は前記ｙを格納するｙ格納部である。

なお、前記１２２～１３３，１３９～１４１はＩＣカード１２０に含まれ、１３４～１３８は補助装置に含まれる。また、１２２～１３１，１３４～１３５は初期化のときのみに動作する。

次に、以上説明した従来のべき乗剰余演算装置の動作をＲＳＡ暗号の復号化を行う場合を例に説明する。なお、ＲＳＡ暗号の復号化演算は前述した通りである。

＜初期化＞

① ＩＣカード内のｐ，ｑ（ＩＣカードの秘密の情報）がそれぞれｐ格納部１２２，ｑ格納部

14

１２３に格納されている。ｎ生成部１２４においてｐとｑの積を計算してｎ公開部１２５に格納する。ｎはこのｎ公開部１２５より広く公開される。ｗｐ，ｗｑ生成部１２６においては前記ｐ，ｑを用いて前記(6)，(7)を満たすｗｐ，ｗｑを生成して格納しておく。

② ＩＣカード内である秘密の数Ｒを決めＲ格納部１２７に格納する。ｒｐ，ｒｑ生成部１２８ではこのＲと前記ｐ，ｑを用いて前記(8)，(9)を満たすｒｐ，ｒｑを生成して格納しておく。

③ ＩＣカード内のｄ（ＩＣカードの秘密の情報）がｄ格納部１２９に格納されている。ｄ′生成部１３０において前記ｄとＲを用いて前記(10)式を満たすｄ′を求める。ｄ′はＩＣカード内のｄ′送信部を通して補助装置内のｄ′受信部１３５に格納される。

④ 補助装置内のｎ受信部１３４は公開されているｎを受信する。

⑤ 補助装置内のｄ′受信部１３５はＩＣカードより送信されたｄ′を受信する。

16

＜繰り返し処理＞

以下の処理は６１２ビットを１ブロックとする暗号文の数だけ繰り返す。

① 暗号文１ブロックをＩＣカード内のｘ格納部に格納する。

② ＩＣカード内のｘ送信部１３３より補助装置内のｘ受信部１３６に暗号文を送信する。

③ 補助装置のべき乗剰余計算部１３７は暗号文ｘ，公開値ｎ，ＩＣカードから受け取ったｄ′を用いて前記(11)の計算を行いｙ′を得る。

④ 補助装置内ｙ′送信部は前記べき乗剰余計算部１３７の出力をＩＣカード内のｙ′受信部１３９に送信する。

⑤ ＩＣカード内のｙ生成部１４０は補助装置が求めたｙ′とＩＣカード内のｗｐ，ｗｑ 生成部１２６，ｒｐ，ｒｑ生成部１２８の格納値を用いて前記(12)の計算を行う。なお、上記の方法で求めたｙは前記(4)を満たすｎ未満の正整数である。それは次のⅰ)～ⅲ)より証明される。

ⅰ) (10)式より次の等式が成り立つ。

$$y = x^{d} \bmod n$$
$$= x^{(d'/R)} \bmod n$$
$$= (x^{d'})^{(R^{(-1)})} \bmod n \quad \cdots\cdots(13)$$

ⅱ) ｎ上の演算である(13)式をｎの素因数であるｐ，ｑ上の演算に分けて計算を行う。

（ｐ上の演算）

$$x^{d'} \bmod p = y' \bmod p \quad ((11)式より)$$
$$R^{(-1)} \bmod (p-1) = rp \quad ((8)式より)$$

従って
$$(x^{d'})^{(R^{(-1)})} \bmod p = (y' \bmod p)^{rp} \bmod p \quad \cdots\cdots(14)$$

（ｑ上の演算）

$$x^{d'} \bmod q = y' \bmod q \quad ((11)式より)$$
$$R^{(-1)} \bmod (q-1) = rq \quad ((9)式より)$$

従って
$$(x^{d'})^{(R^{(-1)})} \bmod q = (y' \bmod q)^{rq} \bmod q \quad \cdots\cdots(15)$$

17

ⅲ) 上記ｐ上の演算結果と上記ｑ上の演算結果とを中国人の剰余定理を用いて結合して(13)式をもとめる。

① ｐ，ｑに対して次の(16)式を満たすｓ，ｔが存在する。

$$p \times s + q \times t = 1 \quad \cdots\cdots(16)$$

② (16)式のｓ，ｔは次のように表すことができる。

$$s = p^{(-1)} \bmod q$$
$$t = q^{(-1)} \bmod p$$

従って(6)，(7)式より

$$q \times t = wp$$
$$p \times s = wq$$

が成り立つ。

③ Ａを任意の算術演算結果とするとき次の(17)式が成り立つ。

$$(A \bmod n) = (A \bmod p) \times wp + (A \bmod q) \times wq \bmod n \quad \cdots\cdots(17)$$

今の場合、$A = (x^{d'})^{(R^{(-1)})}$ である。これに(13)，(14)，(16)をそれぞれ代入すると以下の通りになる。

$$y = \{((y' \bmod p)^{rp} \bmod p) \times wp) + ((y' \bmod q)^{rq} \bmod q) \times wq)\} \bmod n$$

従って(4)式を満たす最終結果は(12)式の結果によって得られることが証明された。

なお、(17)式は以下の(Ⅰ)(Ⅱ)によって証明される。

(Ⅰ) (16)式より、$wp = 1 \bmod p$，$wq = 0 \bmod p$ が成り立つ。

従って(17)式の右辺をｐで除した剰余は $(A \bmod p)$ となる。

(Ⅱ) (16)式より、$wp = 0 \bmod p$，$wq = 1 \bmod p$ が成り立つ。

従って(17)式の右辺をｑで除した剰余は $(A \bmod q)$ となる。

また、補助装置に与えられたデータｘ，ｄ′，ｎのうちｎは公開値であり、ｘは暗号文であるためこれらよりＩＣカードの秘密データを得ることは出来ない。さらに、補助装置がｄ′からｄを求める

19

ためにはｎの素因数分解をすることが必要となるため、ｄの解読は５１２ビットの長語長の数の素因数分解と同等に困難であるといえる。

発明が解決しようとする課題

第２の従来例の場合、繰り返し処理におけるＩＣカードと補助装置との間の通信量はわずか２ブロックである。しかしながら、ＩＣカードが行う(12)式の演算にはｐ，ｑのビット数をそれぞれ２５６ビットとすると、５１２ビットの暗号化に次の演算が必要である。

・２５６ビット幅の乗算剰余（２５６ビットの法上の二項乗算）をｆ（ｒｐ）＋ｆ（ｒｑ）回

ただしｆ（ｒｐ）＝（ｒｐを２進表現したときのビット数）＋（ｒｐを２進表現したときの１の個数）－１とする。

なお、実用的にはこの剰算剰余の回数を小さくするように秘密の数Ｒを選んで処理の高速化を図る。

・５１２ビット幅の乗算剰余（５１２ビットの法上の二項乗算）を　２回

・５１２ビット幅の加算剰余（５１２ビットの法上の二項加算）を　１回

これらの演算を例えばマイクロコンピュータＺ－８０（６ＭＨｚ）を用いて行うとその処理時間4.4秒となる。（ただし、２５６ビット幅の乗算剰余の回数を８回とする）また、ＩＣカードと補助装置との間の通信を９６００ｂｐｓで実現すると仮定した場合その通信時間は0.11秒である。これらを足し合わせると５１２ビットの暗号化に補助装置の演算時間をゼロと考えても4.5秒かかることになる。本発明はかかる点に鑑み、ＩＣカード側の演算を高速化し、その結果としてトータルの暗号化時間を従来より短縮できるべき乗剰余演算装置を提供することを目的とする。

課題を解決するための手段

本発明は、素数ｐと素数ｑの積ｎを法とし、正整数ｄをべき数として入力ｘのべき乗剰余演算を

21

行う装置であり、前記正整数ｄと素数ｐと素数ｑの値を保持し、かつその値が外部から決定あるいは推測できないように構成された第１の計算装置と、第１の計算装置から送出された第１のデータに対して所定の計算を行いその結果を第２のデータとして前記第１の計算装置に送出する第２の計算装置からなり、前記第１の計算装置は前記素数ｐとｑの積ｎと、前記正整数ｄをｐ－１で除した剰余ｄ１と、前記正整数ｄをｑ－１で除した剰余ｄ２を計算してこれらの結果を前記第１のデータとして前記第２の計算装置に送出し、さらに前記第２の計算装置から送出された前記第２のデータを前記素数ｐとｑを用いて結合し、法を前記の数ｎとし、前記正整数ｄをべき数とする入力ｘのべき乗剰余値を求めるものであり、前記第２の計算装置は前記第１の計算装置から送出された前記第１のデータから、前記整数ｎを法とし前記ｄ１をべき数とする前記正整数ｘのべき乗剰余数ｙ１と、前記整数ｎを法とし前記ｄ２をべき数とする前記正整数ｘのべき乗剰余数ｙ２を計算し、この結果を

22 ページ

前記第２のデータとして前記第１の計算装置に対して送出することを特徴とするべき乗剰余演算装置である。

作　用

本発明は前記した構成により、第１の計算装置は最終的に求めたい法ｎ上のべき乗剰余演算を法ｐと法ｑ上の演算に分割して、それぞれを第２の計算装置に計算してもらう。第２の計算装置はｎの素因数ｐ，ｑを知らないので第１の計算装置から与えられたデータより第１の計算装置のＩＣカードの秘密の情報を得ることは困難である。第１の計算装置は第２の計算装置に計算してもらった２つのデータを中国人の剰余定理を用いて結合して所望の結果を得る。

実施例

第１図は本発明の一実施例におけるべき乗剰余演算装置の構成図を示すものである。

第１図において、１はＩＣカード、２は補助装置である。３，４はそれぞれＩＣカードにおける秘密のデータｐ，ｑを格納しているｐ格納部，ｑ

23

格納部、6はpとqの積を計算してnを生成するn生成部、8はnを公開するn公開部である。7はICカードにおける秘密のデータdを格納しているd格納部、8は秘密のデータp，q，dを用いて次の(18)，(19)式を計算してd1，d2を求めるd分割部である。

$$d1 = d \mod (p-1) \quad \cdots\cdots(18)$$

$$d2 = d \mod (q-1) \quad \cdots\cdots(19)$$

9，10は前記d1，d2をそれぞれ補助装置に送信するd1送信部，d2送信部である。11はデータxを格納しているx格納部、12はxを補助装置に送信するx送信部である。13は補助装置内で公開数nを受信するn受信部、14，15，16はそれぞれICカードから送信された前記d1，d2，xを受信するd1受信部，d2受信部，x受信部である。17は13～16に格納されているデータを用いて次の(20)，(21)式を計算してy1，y2を求めるべき乗剰余計算部である。

$$y1 = x \hat{} d1 \mod n \quad \cdots\cdots(20)$$

$$y2 = x \hat{} d2 \mod n \quad \cdots\cdots(21)$$

18，19は前記y1，y2をICカードに送信するy1送信部，y2送信部である。20，21はICカード内で前記y1，y2を補助装置側から受け取るy1受信部，y2受信部である。22は前記y1，y2，p，qを用いて次の(22)，(23)，(24)式を計算してyを生成するy生成部である。

$$u1 = y1 \mod p \quad \cdots\cdots(22)$$

$$u2 = y2 \mod q \quad \cdots\cdots(23)$$

$$y = ((u2+q-u1) \times W \mod q) \times p + u1 \quad \cdots\cdots(24)$$

ただしここでW＝p^(－1) mod qである。

23は前記yを格納するy格納部である。

なお、前記2～12，20～23はICカード1に含まれ、13～19は補助装置に含まれる。また、2～10，13～16は初期化のときのみに動作する。

次に、以上説明した本実施例のべき乗剰余演算装置の動作を、従来例と同様にRSA暗号の復号化を行う場合を例に説明する。

25

＜初期化＞

① ICカード内のp，q（ICカードの秘密の情報）がそれぞれp格納部3，q格納部4に格納されている。n生成部6においてp，qの積を計算してn公開部6に格納する。nはこのn格納部により広く公開される。

② ICカード内のd（ICカードの秘密の情報）がd格納部7に格納されている。d分割部8においてdを前記(18)式を満たすd1，d2を求める。そしてdの代わりにd1，d2を送信部9，10を通して補助装置に送信する。

③ ICカード内の秘密の情報p，qを用いてW＝p^(－1) mod qを計算しておく。

④ 補助装置内のn受信部13は公開されているnを受信する。

⑤ 補助装置内のd1，d2受信部はICカードより送信されたd1，d2を受信する。

＜繰り返し処理＞

以下の処理は512ビットを1ブロックとする暗号分の数だけ繰り返す。

26 ページ

① 暗号文1ブロックをICカード内のx格納部に格納する。

② ICカード内のx送信部12より補助装置内のx受信部16に暗号文xを送信する。

③ 補助装置のべき乗剰余計算部17は暗号文x，公開値n，ICカードから受け取ったd1，d2を用いて前記(20)，(21)の演算を行いy1，y2を求める。

④ 補助装置内のy1，y2送信部は前記べき乗剰余計算部17の出力をICカード内のy1，y2受信部に送信する。

⑤ ICカード内のy生成部22は補助装置が求めたy1，y2をICカードの秘密のデータp，qを用いて前記(22)，(23)，(24)式を計算する。

なお、上記の方法で求めたyは

$$y = x \hat{} d \mod n \quad \cdots\cdots(25)$$

を満たすn未満の正整数である。それは次のi)ii)より証明される。

i) n上の演算である(25)式をnの素因数p，q上の演算に分けて計算を行う。

27

（ｐ上の演算）

$$x^{d} \bmod p = x^{(d \bmod (p-1))} \bmod p = x^{d_1} \bmod p \quad (18)\text{式より} = y_1 \bmod p \quad (20)\text{式より} = u_1 \quad (22)\text{式より} \quad \cdots\cdots(26)$$

（ｑ上の演算）

$$x^{d} \bmod q = x^{(d \bmod (q-1))} \bmod q = x^{d_2} \bmod q \quad (19)\text{式より} = y_2 \bmod q \quad (21)\text{式より} = u_2 \quad (23)\text{式より} \quad \cdots\cdots(27)$$

(ii) 上記求めたｐ上の演算結果とｑ上の演算結果中国人の剰余定理を用いて結合する。

① ｐ，ｑより次の(28)を満たすＷを求める。

$$W = p^{(-1)} \bmod q \quad \cdots\cdots(28)$$

② Ａを任意の算術演算結果とする時、次の(29)式が成り立つ。

$$A \bmod n = [\{(A \bmod q) + q - (A \bmod p)\} \times W \bmod q] \times p + (A \bmod p) \quad \cdots\cdots(29)$$

今の場合、Ａ＝ｘ^ｄである。

これに(25)～(27)を代入すると(24)式が成り立つことが証明される。

なお、(29)式を計算することによって(26)式を満たすｙが求められることは次の(i)～(iii)により証明される。

(i) (29)式の右辺はｎ未満の値である。

〔理由〕

$\{(A \bmod q) + q - (A \bmod p)\} \times W \bmod q \} \leq q-1$ $(A \bmod p) \leq p-1$ であることより

従って(29)式の右辺 $\leq (q-1) \times p + (p-1) = p \times q - 1 < n$

29

(ii) (29)式右辺の法ｐにおける値が（Ａ mod p）となることは自明である。

(iii) (29)式右辺の法ｑにおける値が（Ａ mod q）となる。

〔理由〕

(28)式のＷを(29)式に代入して法ｑにおける値を求めると

$\{(A \bmod q) + q - (A \bmod p)\} \times p^{(-1)} \times p + (A \bmod p) \bmod q = (A \bmod q)$

となる。

また、ｄ１，ｄ２よりｄを求めるためにはｎの素因数分解をすることが必要となるため、素因数ｐ，ｑを知らない補助装置にとってｄの解読は５１２ビットの長語長の数の素因数分解と同等に困難であると言える。この点では従来の第２の実施例と同じ安全性であると言える。

繰り返し処理時におけるＩＣカードと補助装置との間の通信量はＩＣカードから補助装置に１ブロック、補助装置からＩＣカードに２ブロックの

30

計３ブロックである。この通信量は９６００bpsで通信を行うと仮定したとき０.１６秒に相当する。また、ＩＣカードが行う(22)～(24)の演算には次の演算が必要である。

・２５６ビット幅の剰余演算を　２回
・２５６ビットの乗算剰余演算を１回
・２５６ビットの乗算を　１回
・２５６ビットの加算を　２回
・５１２ビットの加算を　１回

これらの演算を例えばマイクロコンピュータＺ－８０（６MHz）を用いておこなうとその処理時間は約０.９７５秒となる。ただし、２５６ビットの剰余演算の処理時間を０.１７５sec／１回、２５６ビットの乗算時間を０.１７５sec／１回、２５６ビットの乗算剰余の演算時間を０.３５sec／１回、２５６ビットの加算時間を０.０２５秒／１回、５１２ビットの加算時間を０.０５秒／１回としている。従って、通信時間とＩＣカードにおける処理時間を足し合わせると１.１３５秒になる。従来例と同様に補助装置の演算時間をゼロと

31

考えると1.136秒で512ビットの暗号化が実行されることになる。

以上のように、本実施例によれば通信量は従来よりも多少増加するが、ICカード側の演算を軽減することによってトータルとして従来例の約4倍の速度アップを得ることができる。

なお、この実施例においては(24)式に示した効率的な中国人の剰余定理を用いたが、従来例と同様(12)式に示した式で法p上の演算結果と法q上の演算結果を結合しても良い。

発明の効果

以上説明したように、本発明によれば繰り返し処理において第1の計算装置は最終的に求めたいべき乗剰余演算の「べき乗」の部分を全部実行してもらう。そのため、第1の計算装置におき、中国人の剰余定理を用いて第2の計算装置の行った演算結果を結合する際、その演算の中にはべき乗剰余演算が含まれていない。これによって、第1の計算装置の負担する演算が従来（第2の従来例）に比べて4倍以上軽減する。

33

の従来例のブロック図である。

1，100，120……ICカード、2，101，121……補助装置、3，102，122……p格納部、4，103，123……q格納部、5，104，124……n生成部、6，106，125……n公開部、7，106，129……d格納部、11，110，132……x格納部、17，115，137……べき乗剰余計算部、23，119，141……y格納部。

代理人の氏名　弁理士　栗　野　重　孝　ほか1名

第2の計算装置の行う演算量はべき乗のビット数を考えると従来と同等であることが分かる。

また、第1の計算装置と第2の計算装置の間の通信量は従来の1.5倍になるが、通信速度を例えば9600bpsと考えると従来例との通信時間の差は非常に小さい。

以上のことより、処理時間のトータルとしては1回の繰り返しについて従来の4倍の高速化が達成できている。

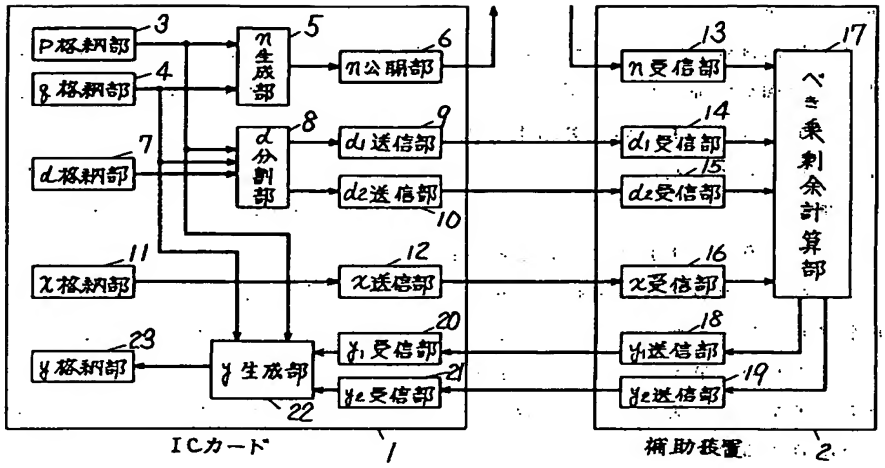
第1の計算装置の保持している秘密データの安全性については、第2の計算装置が得ているd1，d2からdを得る困難さがnの素因数分解を行う困難さと同等であると考えられるため、nを512ビット程度にすることによって保証される。この点は従来と同じである。

これらのことより本発明の実用的効果は大きい。

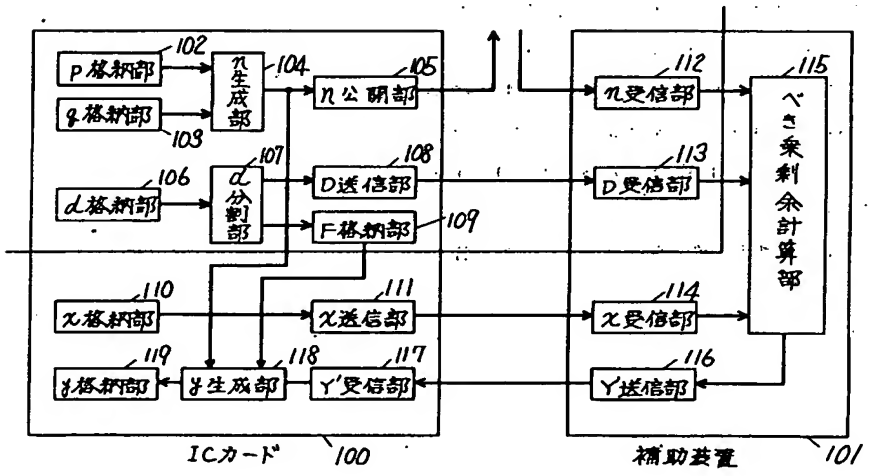
4、図面の簡単な説明

第1図は本発明における一実施例のべき乗剰余演算装置のブロック図、第2図は第1の従来例のべき乗剰余演算装置のブロック図、第3図は第2

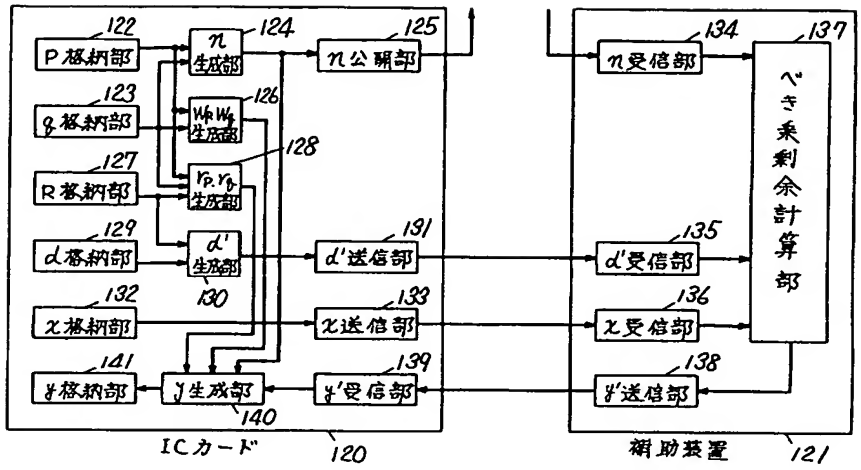
第 1 図


P格納部
g格納部
d格納部
χ格納部
γ格納部
n生成部
α分割部
γ生成部
n公開部
d1送信部
d2送信部
χ送信部
γ1受信部
γ2受信部
n受信部
d1受信部
d2受信部
χ受信部
γ1送信部
γ2送信部
べき乗剰余計算部
ICカード
1
補助装置
2

第 2 図


P格納部
g格納部
d格納部
χ格納部
γ格納部
n生成部
α分割部
γ生成部
n公開部
D送信部
F格納部
χ送信部
γ'受信部
n受信部
D受信部
χ受信部
γ'送信部
べき乗剰余計算部
ICカード
100
補助装置
101

第 3 図


122
P格納部
124
n 生成部
125
n公開部
123
g格納部
126
W_A W_B 生成部
128
r_P r_Q 生成部
127
R格納部
129
d格納部
d' 生成部
130
131
d'送信部
132
x格納部
133
x送信部
141
y格納部
y生成部
140
139
y'受信部
ICカード
120
134
n受信部
137
べき乗剰余計算部
135
d'受信部
136
x受信部
138
y'送信部
補助装置
121